# Protect Root / Global Admins Account

## Objective

Protect root or master account used to establish the cloud service.

## Key Considerations

* [ ] Implement multi-factor authentication (MFA) mechanism for root/master account.
* [ ] Document a break glass emergency account management procedure. Including names of users with root or master account access.
* [ ] Obtain signature from Departmental Chief Information Officer (CIO) and Chief Security Officer (CSO) to confirm acknowledgement and approval of the break glass emergency account management procedures.
* [ ] Implement a mechanism for enforcing access authorizations.
* [ ] Configure appropriate alerts on root/master accounts to detect a potential compromise, in accordance with the [GC Event Logging Guidance](https://www.gcpedia.gc.ca/gcwiki/images/e/e3/GC_Event_Logging_Strategy.pdf)

## Validation

* [ ] Confirm policy for MFA is enabled through screenshots and compliance reports.
* [ ] Confirm that an attestation letter of the emergency break glass procedure has been signed by the Departmental CIO and CSO.

## Additional Considerations

* [ ] Leverage enterprise services such as Administrative Access Control System (AACS) for Privileged Access Management (PAM), Attribute-based access control (ABAC).

## Applicable Service Models

* IaaS, PaaS, SaaS

## References

1. [SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.3
2. CSE Top 10 #3
3. Refer to the [Recommendations for Two-Factor User Authentication Within the Government of Canada Enterprise Domain](https://intranet.canada.ca/wg-tg/rtua-rafu-eng.asp)
4. Refer to the following [template](https://gcconnex.gc.ca/file/view/55010566/break-glass-emergency-account-procedure-departments-can-use-to-develop-their-emergency-access-management-controls-for-cloud?language=en) for an example of a break glass emergency account management procedure.
5. Refer to the [GC Event Logging Guidance](https://www.gcpedia.gc.ca/gcwiki/images/e/e3/GC_Event_Logging_Strategy.pdf)
6. Related security controls: AC‑2, AC‑2(1), AC‑3, AC‑5, AC‑6, AC‑6(5), AC‑6(10), AC‑7, AC‑9, AC‑19, AC‑20(3), IA‑2, IA‑2(1), IA‑2(2), IA‑2(11), IA‑4, IA‑5, IA‑5(1), IA‑5(6), IA‑5(7), IA‑5(13), IA‑6, IA‑8